# 無線LAN控制器啟動顯示頁面重新導向組態範例

## 目錄

簡介
必要條件
需求
採用元件
慣例
背景資訊
網路設定
設定
步驟1.配置WLC以通過Cisco Secure ACS伺服器進行RADIUS身份驗證。
步驟2.為管理和操作部門配置WLAN。
步驟3.配置Cisco Secure ACS以支援啟動顯示頁面重定向功能。
驗證
疑難排解
相關資訊

## <u>簡介</u>

本檔案介紹如何在無線LAN控制器上設定啟動顯示頁面重新導向功能。

## <u>必要條件</u>

### <u>需求</u>

嘗試此組態之前,請確保符合以下要求:

- •瞭解LWAPP安全解決方案
- 瞭解如何配置Cisco Secure ACS

### <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 執行韌體版本5.0的Cisco 4400系列無線LAN控制器(WLC)
- 思科1232系列輕型接入點(LAP)
- •執行韌體版本4.1的Cisco Aironet 802.a/b/g無線使用者端配接器
- 運行版本4.1的Cisco Secure ACS伺服器
- •任何第三方外部Web伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

### <u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

## <u>背景資訊</u>

啟動顯示頁面Web重新導向是無線LAN控制器版本5.0中引入的功能。使用此功能,使用者在 802.1x驗證完成後將被重定向到特定網頁。使用者開啟瀏覽器(設定為預設首頁)或嘗試存取 URL時,會發生重新導向。重新導向網頁完成後,使用者會獲得網路的完整存取許可權。

您可以在遠端驗證撥入使用者服務(RADIUS)伺服器上指定重新導向頁面。應將RADIUS伺服器設定 為在802.1x驗證成功時將思科av配對url-redirect RADIUS屬性傳回到無線LAN控制器。

啟動顯示頁面Web重新導向功能僅適用於針對802.1x或WPA/WPA2第2層安全性設定的WLAN。

### <u>網路設定</u>

在以下範例中,Cisco 4404 WLC和Cisco 1232系列LAP透過第2層交換器連線。Cisco Secure ACS伺服器(充當外部RADIUS伺服器)也連線到同一台交換機。所有裝置都位於同一個子網中。

LAP最初註冊到控制器。您必須建立兩個WLAN:一個用於**管理部**使用者,另一個用於**運營部**使用 者。兩個無線LAN都使用WPA2/AES(EAP-FAST用於身份驗證)。兩種WLAN均使用啟動顯示頁 面重新導向功能將使用者重新導向到適當的首頁URL(在外部Web伺服器上)。

本檔案會使用以下網路設定:



Cisco Secure ACS server

WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cioco Socuro ACS convor ID address	10 77 244 106
Cisco Secure ACS server in address	10.77.244.190

Subnet Mask used in this example 255.255.255.224

下一節說明如何為此設定配置裝置。

## <u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

**註:使**用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

完成以下步驟,將裝置設定為使用啟動顯示頁面重新導向功能:

- 1. <u>配置WLC以通過Cisco Secure ACS伺服器進行RADIUS身份驗證。</u>
- 2. <u>為管理部門和運營部門配置WLAN。</u>
- 3. <u>配置Cisco Secure ACS以支援啟動顯示頁面重定向功能。</u>

### 步驟1.配置WLC以通過Cisco Secure ACS伺服器進行RADIUS身份驗證。

需要設定WLC,才能將使用者認證轉送到外部RADIUS伺服器。

完成以下步驟,設定外部RADIUS伺服器的WLC:

- 1. 從控制器GUI中選擇**Security**和**RADIUS Authentication**,以顯示「RADIUS Authentication Servers」頁面。
- 2. 按一下New以定義RADIUS伺服器。
- 3. 在RADIUS Authentication Servers > New頁面上定義RADIUS伺服器引數。這些引數包括 :RADIUS伺服器IP位址共用金鑰連線埠號碼伺服器狀態

					Sa <u>v</u> e Co	nfiguration   Eing	Logout   Befresh
CISCO	MONITOR WLANS CONTR	ROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	_
Security	RADIUS Authentication	Servers > New				< Back	Apply
Security • AAA General • RADIUS Authentication Accounting • TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies • Local EAP • Priority Order • Access Control Lists • Wireless Protection Policies • Web Auth • Advanced	RADIUS Authentication Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Server Timeout Network User Management IPSec	Servers > New  I I III III III IIII IIII IIII IIII	IPS customens	and requires a ke	y wrap compliant	< Back	Apply
		- //					

本文檔使用IP地址為10.77.244.196的ACS伺服器。

4. 按一下「Apply」。

### 步驟2.為管理和操作部門配置WLAN。

在此步驟中,您配置客戶端用於連線無線網路的兩個WLAN(一個用於管理部門,另一個用於運營 部門)。

管理部門的WLAN SSID將為Admin。操作部門的WLAN SSID為操作。

使用EAP-FAST驗證以啟用WPA2作為WLAN上的第2層安全機制,並使用Web策略 — 啟動顯示頁 面Web重新導向功能作為第3層安全方法。

完成以下步驟即可設定WLAN及其相關引數:

- 1. 從控制器的GUI中按一下「**WLANs**」,以顯示「WLANs」頁面。此頁面列出控制器上存在的 WLAN。
- 2. 按一下New以建立一個新的WLAN。

- ahaha -						Sage Co	infiguration Eing	Logout Befresh
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN	×					
Advanced	Profile Name	Admin						
	WLAN SSID	Admin						

- 3. 在WLANs > New頁面上輸入WLAN SSID名稱和配置檔名稱。
- 4. 按一下「Apply」。
- 5. 首先為管理部門建立WLAN。建立新的WLAN後,系統會顯示新WLAN的WLAN > Edit頁面。 在此頁面上,您可以定義此WLAN的特定各種引數。這包括常規策略、安全策略、QOS策略和 高級引數。
- 6. 在General Policies下,勾選Status覈取方塊以啟用WLAN。

e aludue -							Saye C	onfiguration Eing	Logout <u>R</u> efre
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
WLANs	WLANs > I	Edit						< Back	Apply
WLANS WLANS Hadvanced	WLANS > I General Profile N Type SSID Status Security Radio Po Interfac Broadca	Edit Secur Aame Policies olicy e sst SSID	ity QoS Admin WLAN Admin ☑ Enable Splash- (Modificati All admin ☑ Enable	Advanced ad Page-Web-R ons done unde	edirect[WPA2 r security tab	2][Auth(802.1X)] will appear after ap	l oplying the chan	< Back	Apply

- 7. 按一下Security頁籤,然後按一下Layer 2頁籤。
- 8. 從Layer 2 Security下拉選單中選擇WPA+WPA2。此步驟為WLAN啟用WPA身份驗證。
- 9. 在WPA+WPA2引數下, 選中WPA2 Policy和AES Encryption覈取方塊。

- ahaha-				Sa <u>v</u> e Co	infiguration Ping	Logout   Befre
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	_
WLANS WLANS WLANS Advanced	WLANS > Edit         General       Security       QoS         Layer 2       Layer 3       AAA Ser         Layer 2       Layer 3       AAA Ser         Layer 2       Layer 3       AAA Ser         MAC Filtering       MAC Filtering         WPA+WPA2 Parameters       MAC Filtering         WPA2 Policy       Image: Compared and the second and th	Advanced vers TKIP			< Back	Apply

- 10. 從Auth Key Mgmt下拉選單中選擇**802.1x**。此選項為WLAN啟用具有802.1x/EAP身份驗證和 AES加密的WPA2。
- 11. 按一下Layer 3 Security頁籤。
- 12. 選中Web Policy框,然後按一下Splash Page Web Redirect單選按鈕。此選項可啟用啟動顯示頁面Web重新導向功能。

a duala a second							Sa <u>v</u> e Co	onfiguration   Ping	Logout   <u>R</u> efre
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANS WLANS WLANS Advanced	WLANS> General Layer Laye C p C c C p C c C p C c	WLANS Edit Secur 2 Layu or 3 Security Web Policy Web Policy wuthenticatio conditional 1 conditional 1 conditional 1 conditional 2	ity QoS er 3 AAA Se r None 2 on Web Redirect Web Redirect in None	Advanced rvers	SECONDIA	MQNAGEMENT		< Back	Apply

### 13. 按一下AAA Servers頁籤。

14. 在Authentication Servers下,從Server 1下拉選單中選擇適當的伺服器IP地址。

abab	Sa <u>v</u> e Configuration   <u>P</u> ing   Logou	nt i <u>B</u> et
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit Ap	ply
* WLANS	General Security QoS Advanced	
WLANs	Layer 2 Layer 3 AAA Servers	
Advanced	*	
	Select AAA servers below to override use of default servers on this WLAN	
	Radius Servers LDAP Servers	
	Authentication Servers Accounting Servers Server 1 None 💌	
	Enabled Server 2 None 💌	
	Server 1P:10.77.244.196, Port:1812 None Server 3 None S	
	Server None Y	
	Server None None V	
	Local EAP Authentication	
	Local EAP Authentication Enabled	
	Authentication priority order for web-auth user	

在本示例中,10.77.244.196用作RADIUS伺服器。

- 15. 按一下「Apply」。
- 16. 重複步驟2至15,為運營部門建立WLAN。WLANs頁面列出您建立的兩個WLAN。

						onfiguration Ping Lo	gout   <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER WIREL	ESS SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs						New
✓ WLANS WLANS	Profile Name	Туре	WLAN SSID		Admin Status	Security Policies	
Advanced	Admin	WLAN	Admin		Enabled	[WPA2][Auth(802.1X)],	Splash-Page
	Operations	WLAN	Operations		Enabled	[WPA2][Auth(802.1X)],	Splash-Page

請注意,安全策略包括啟動顯示頁面重新導向。

### 步驟3.配置Cisco Secure ACS以支援啟動顯示頁面重定向功能。

下一步是為此功能設定RADIUS伺服器。RADIUS伺服器需要執行EAP-FAST驗證以驗證使用者端憑 證,並在成功驗證後,將使用者重新導向至Cisco av配對*url-redirect* RADIUS屬性中指定的網址 (在外部Web伺服器上)。

#### 配置Cisco Secure ACS進行EAP-FAST身份驗證

注意:本檔案假設無線LAN控制器作為AAA使用者端新增到Cisco Secure ACS。

完成以下步驟,以便在RADIUS伺服器中設定EAP-FAST驗證:

1. 在RADIUS伺服器GUI中按一下**System Configuration**,然後在System Configuration頁面中選 擇**Global Authentication Setup**。

CiscoSecure ACS - 1	Microsoft Internet Explorer	18×
Ele Edt Yew Fa	vorites Iools Help	Links <sup>30</sup> Oose
Address a http://127.	0.0.1:1065/	• 🔁 •
Cites Systems	System Configuration	X
User Setup Setup Setup Setup Setup Setup Components Configuration Surtern Configuration Configuration	Security Service Control Security Service Control Security Service Control Security Service Management Control Service Management ACS Decide Service Management ACS Certificate Setup Security Security Setup Security Security Setup Security Security Sec	Service Control     Lessins     Date Format Control     Lessins     Date Format Control     Ads Internat Control     Ads Internat Control     Ads Internat Control     Ads Internation     Ads Internation     More Service Management     IP Profit Address Reservery     IP Profit Address Reservery     IP Profit Address Reservery     IP Profit Address Reservery     Sichal Anthontication Configuration     Ads Contificate Setup     Sichal Anthontication Configuration
Control User Databases Patients Profiles Profiles Reports and Activity Documentation	P Back to Hulp	Service Control Select to open the page from which you can stop or restart Circo Secure ACS services. [Reck to Tro] Select to configure various Circo Secure ACS reports and customire the type of information that is logged. [Reck to Tro] Date Format Control Select to configure the date format, either month/day/year or day/month/year, for CSV files and Service Logs and in the GUI. [Back to Tro]
		internet
start 19 8	CiscoSecure ACS - Mic	9 7:57 PM

2. 在Global Authentication setup頁中,按一下**EAP-FAST Configuration**以轉到EAP-FAST設定頁

o

ElscoSecure AES -	Microsoft Internet Explorer			Links * 🎥
ress ) http://127.	0.0.1:1065/		]	• • •
Crees Systems	System Configuration	-		X
Diller 1	EAP Configuration	Help		î
Group Setup Setup Shared/rofile Components	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation	Use this protocoli • CAP Com • PEAP • CAP FAX	spage to specify settings for various authenticution s. <del>Demation</del> XX	
Network Configuration System Configuration	Allow EAP-TLS Select one or more of the following options: E Certificate SAN comparison	<ul> <li>CAPLIDS</li> <li>LEAP</li> <li>CAPLINE</li> <li>APLIAP</li> <li>10:0000</li> </ul>	i Report Diversit P.Configuration	
Administration Centrel External User Databases	EAP-TLS session timeout (minutes): 120	EAP Coal EAP is a suthers	<b>figeration</b> iffeetide request-response protocol for arbitrary cation information (RFC 2204), EAP is layered on top of subsend exception of 1000 March 1 and FADIDA and embedded	,
Porture Validation Network Access Profiles	Cisco client initial message: PEAP session timeout (minutes): 120 Enable Fast Reconnect: R	Iback to PEAP	"authantication" types. -Tup]	
Activity Online Documentation	EAP-FAST EAP-FAST Configuration	PEAP is	the outer layer protocol for the secure tunnel.	
	EAP-TLS I Allow EAP-TLS Select one or more of the following options: I Certificate SAN comparison	Allow Education	(AF is a contribute-based sublembiostion protocol. AEAP Cable can eccur only after you have completed the required the ACS Certificate Setup page. AD-MSCHADV2 — Use to enable EAD-MSCHADV2 within ic ution. Enable this protocol for any reportany that supp is unch as Microsoft AD, and the ACS Internal Database	MS PEAP orts MS-
	Submit Submit + Restart Cancel	1		
			Internet	
tart 🔂 🥭	CiscoSecure ACS - Mic			📑 7:58 PM

3. 在EAP-FAST設定頁面中,選中**Allow EAP-FAST**覈取方塊以便在RADIUS伺服器中啟用EAP-FAST。

Cisco Systems	System Configuration		0
db.db.	EAP-FAST Configuration	1	Help
User			
Tottop	EAD-EAST Settless		EAP-FAST Configuration Page
Group Setup	EAP-FAST aettings	<b>1</b>	Use this page to configure EAP-FAST authentication settings.
SharedProfile	EAP-FAST	181	GAD-GAST Setting
Components	M Allow EAP-FAST	108	Chent initial message
Network	Active master key TTL 1 months	191	Authority ID Infe
Contrigue action	Retired master key TTL 3 months 💌	128	<ul> <li>Allow assignment in hand PAC previousing</li> <li>Allow astheritz at a fire hand PAC previousing</li> </ul>
System Configuration			<ul> <li>Afters machine authentication</li> </ul>
	Turinel PAC TTL 1 weeks	198	<ul> <li>Allow stateless searches resource</li> </ul>
Configuration	Client initial message: tacwebacs	110	Control and and an article and a second and a second and a second at a se
Administration	Authority ID Info: tacwebacs	181	<ul> <li>EAP-TLS session timeset (minutes)</li> </ul>
entrel	E they accuracy in-band DAC equilibrium	10	CAP-FAST master server     Actual FAP-FAST server status
bdernal User	F allow anonymous in-band PAC provisioning	121	
Pabates	C Allow authenticated in-band PAC provisioning	100	EAP-FAST Settings
alidation	Accept client on authenticated provisioning	108	Allow EAP-FAST-To enable EAP-FAST authentication, select this check
	Require client certificate for provisioning	121	ben.
offier	C Allow Machine Authentication	128	
I heather	Machine PAC TTL 1 weeks	-	<ul> <li>Active Haster Key TILEnter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the</li> </ul>
Lotivity	E tilen Statelers service service		time to live (TTL) defined for the Master Key expires, the master key is considered retired and a new master key is generated.
Inline	1.1 Allow Stateless session resume		
Documentation	Authorization PAC TTL 1 hours		<ul> <li>Retired master key TIL - Enter a value for the amount of time that PACs</li> </ul>
	Allowed inner methods		authentication. When an end-user client gains network access using a PAC
	R EAP-GTC		based on a retired master key, ACS sends a new PAC to the end-user client.
	R EAP-MSCHAPv2		<ul> <li>Tunnel PAC TIL - Enter a value for the amount of time that a PAC is used</li> </ul>
	EAP-TLS		Before it expires and must be replaced. If the master key used to generate the Tonnel PAC has not expired, new PAC departure and accimentation
	Cubmit Cubmit + Bartaut Canad	- 22	automatic. If the master key used to generate the Tunnel PAC expired.
	Submit Submit + Restart Cancel		automatic or manual provisioning must be used to provide the end-user client with a new PAC.

- 4. 根據需要配置活動/已停用主金鑰TTL(生存時間)值,或將其設定為預設值(如本例所示)。 Authority ID Info欄位表示此ACS伺服器的文本標識,終端使用者可以使用該標識來確定對其進 行身份驗證的ACS伺服器。必須填寫此欄位。Client initial display message欄位指定要傳送給 使用EAP-FAST客戶端進行身份驗證的使用者的消息。最大長度為40個字元。僅當終端使用者 客戶端支援顯示時,使用者才會看到初始消息。
- 5. 如果您希望ACS執行匿名帶內PAC調配,請選中允許匿名帶內PAC調配覈取方塊。
- 6. Allowed inner methods選項確定哪些內部EAP方法可以在EAP-FAST TLS隧道內運行。對於匿 名帶內調配,必須啟用EAP-GTC和EAP-MS-CHAP以實現向後相容性。如果選擇Allow anonymous in-band PAC provisioning(允許匿名帶內PAC調配),則必須選擇EAP-MS-CHAP(零階段)和EAP-GTC(第二階段)。
- 7. 按一下「Submit」。注意:有關如何使用匿名帶內PAC調配和身份驗證帶內調配配置EAP FAST的詳細資訊和示例,請參閱<u>使用無線LAN控制器和外部RADIUS伺服器配置的EAP-</u> <u>FAST身份驗證示例</u>。

#### 配置使用者資料庫並定義url-redirect RADIUS屬性

此示例將無線客戶端的使用者名稱和密碼分別配置為User1和User1。

完成以下步驟即可建立使用者資料庫:

- 1. 從導航欄中的ACS GUI中選擇User Setup。
- 2. 建立一個新的無線使用者,然後按一下Add/Edit以轉到此使用者的「編輯」頁。



3. 在User Setup Edit頁中,配置Real Name和Description以及Password設定,如本例所示。本 文檔使用ACS內部資料庫進行口令驗證。

http://127.	.0.0.1:1065/	
Statema	User Setup	
	Edit	Help
er hup top areditrofile moments twork figuration them figuration	User: User1 (New User)  Account Disabled  Supplementary User Info Real Name Description	Account Disabled     Onletting, a Operance     Suplementary Days Info     Camp to which the oper is assigned     Callback     Clent IP Address Assignment     Advanced Sattleme     Network Account Sattleme     Man Second Sattleme     Occursted
ministration Ntrol Sernal User Abases Shore Sidation Modik Access Siles	User Setup ? Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not charked )	Advanced LALAGE Stations     LALAGE Stations     LALAGE Leading Control     LALAGE Leading Control     LALAGE Control Control     LALAGE Stations     LALAGE Stations for Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application     LALAGE Control of the Not treach Device Nonseement Application
ports and tivity	Confirm Password Confirm Password Confirm Password Confirm Password Confirm Password Confirm Password Submit Cancel	Account Disabled Status Select the Account Disabled check box to disable this account cle- the check box to enable the account. [Back to Top] Deleting a Username The Delete button appears only when you are editing an existing ost- count, not when you are adding a new user account. To delete the current user account from the database, click <b>Delete</b> . When asked to confirm your action. click <b>Of</b> .

- 4. 向下滾動頁面以修改RADIUS屬性。
- 5. 選中[009\001] cisco-av-pair覈取方塊。
- 6. 在[009\001] cisco-av-pair編輯框中輸入此Cisco av-pair,以指定將使用者重定向到的URL:urlredirect=http://10.77.244.196/Admin-

### Login.html

Cisco Systems	User Setup	[
adducad hu	(useu iur benuPass anu benuAutri cirents such as routers)	Hetp
User Setup	Password	Account Disabled
Setup	Password	Onleting a Unername     Supplementary User Info     Description
Shared Profile Components	Cisco Airespace RADIUS Attributes	Converte to which the user is assigned     Callback
Network Configuration	[14179/005] Aire-Interface-Name	Chent IP Address Assignment     Advanced Settings
System Configuration		Has Session     Usage Owners
Configuration		Account Disable     Dorrelo ed able ACLs     Advanced TACACLS
Administration Centrel	Cisco IOS/PIX 6.x RADIUS Attributes	TACACS - Enable Central     TACACS - Enable Passward
Databases	R [009\001] cisco-av-pair	TACACS - Outbound Passment     TACACS - Shell Command Artherization     Ecompard Authorization for Network During Management Applications
verse Posture Validation	url- redirect=http://10.77.244.196/	TACACS - Unknown Services     IETE RADRUS Attributes
Network Access Profiles	Kdmin-Hogin.html	RADEUS Vendor-Saecific Attributes
Reports and Activity		Account Disabled Status
Documentation		Select the Account Disabled check box to disable this account clear the check box to enable the account.
	Back to Help	[hash to Top]
	•	Deleting a Username

Submit Delete Cancel

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the

這是管理部門使用者的首頁。

- 7. 按一下「Submit」。
- 8. 重複此過程以新增User2(操作部門使用者)。
- 9. 重複步驟1到6,以便向資料庫中新增更多的管理部門使用者和操作部門使用者。注意 :RADIUS屬性可在Cisco Secure ACS上的使用者級別或組級別進行配置。

## 驗證

為了驗證配置,請將管理部門和運營部門的WLAN客戶端與其相應的WLAN相關聯。

當管理員部門的使用者連線到Wireless LAN Admin時,系統將提示該使用者輸入802.1x憑證(在本 例中為EAP-FAST憑證)。使用者提供憑證後,WLC會將這些憑證傳遞到Cisco Secure ACS伺服器 。Cisco Secure ACS伺服器根據資料庫驗證使用者憑證,並在身份驗證成功後將url-redirect屬性返 回到無線LAN控制器。身份驗證在此階段完成。

😤 Cisco Aironet Desktop Utilit	y - Current Profile: Admin		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
Profile Name:	Admin		
Link Status:	Not Associated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server Based Authentication:	None	Data Encryption: AES	
IP Address:	10.77.244.221		
Signal Strength		Good	
		Advanced	D

當使用者開啟Web瀏覽器時,系統會將使用者重定向到管理部門的首頁URL。(此URL會透過 cisco-av-pair屬性傳回WLC)。重新導向後,使用者會獲得網路的完整存取權限。以下截圖:



當操作部門的使用者連線到WLAN Operations時,會發生相同的事件序列。

🖻 Cisco Aironet Desktop Utility - Current Profile: Operations 🛛 🔹 🛛					
Action Options Help					
Current Status Profile Management	Diagnostics				
CISCO SYSTEMS					
utilituutilituu Profile Name:	Operations				
Link Status:	Authenticated	Network Type: Infrastructure			
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149			
Server Based Authentication:	EAP-FAST	Data Encryption: AES			
IP Address:	10.77.244.221				
Signal Strength:		Good			
		Advanced			



## <u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</u>。

您可以使用以下命令對配置進行故障排除。

• Sho WLA Pro Net	DW WIAN WIAN_IG — 顯示符定WLAN的Web重新導回功能的狀態。以卜是範例: N Identifier1 file NameAdmin work Name (SSID)
Web Web	Based Authentication Disabled -Passthrough Disabled
Con	ditional Web Redirect
Spl	ash-Page Web Redirect Enabled
• det	oug dot1x events enable — 啟用802.1x資料包消息的調試。以下是範例:
Fri	Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
	mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri	Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
	mobile 00:40:96:ac:dd:05
Fri	Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
	mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri	Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
	mobile 00.40.96.ac.dd.05
<b>F</b> ri	The $20, 10, 27, 16, 2008$ : $00, 40, 96, 20, 200$ Setting re-suth timeout to 1800
LTT	rep 29 10-27-10 2000. 00-40-90-ac-dd-05 Setting re-addir timeout to 1000
<b>D</b> -1	Seconds, got from whan config.
Fri	Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
Fri	setting dotlx reauth timeout = 1800 Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry for station 00:40:96:ac:dd:05 (RSN 2)

ALL UN AL

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
     to PMKID cache for station 00:40:96:ac:dd:05
 Fri Feb 29 10:27:16 2008: New PMKID: (16)
 Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
     fb fa 8e 3c
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
     lifetime can take care of same.
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
     00:40:96:ac:dd:05 (EAP Id 17)
 Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16)
 Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
     fb fa 8e 3c
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
     mobile 00:40:96:ac:dd:05
     state INITPMK (message 1), replay counter 00.00.00.00.00.00.00
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
     in Authenticating state for mobile 00:40:96:ac:dd:05
• debug aaa events enable — 啟用所有aaa事件的調試輸出。以下是範例:
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
     Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
     00:40:96:ac:dd:05-00:00
 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
     RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
     Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
     00:40:96:ac:dd:05-00:00
 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
     RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
     'http://10.77.244.196/Admin-login.html' set
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
     station 00:40:96:ac:dd:05
 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
     00:40:96:ac:dd:05
        source: 4, valid bits: 0x0
        gosLevel: -1, dscp: 0xfffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
        vlanIfName: '', aclName: '
```

### 相關資訊

- 思科無線LAN控制器組態設定指南5.0版
- 無線 LAN 控制器 Web 驗證組態範例
- 使用無線 LAN 控制器的外部 Web 驗證組態範例
- 無線支援頁面
- 技術支援與文件 Cisco Systems

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。